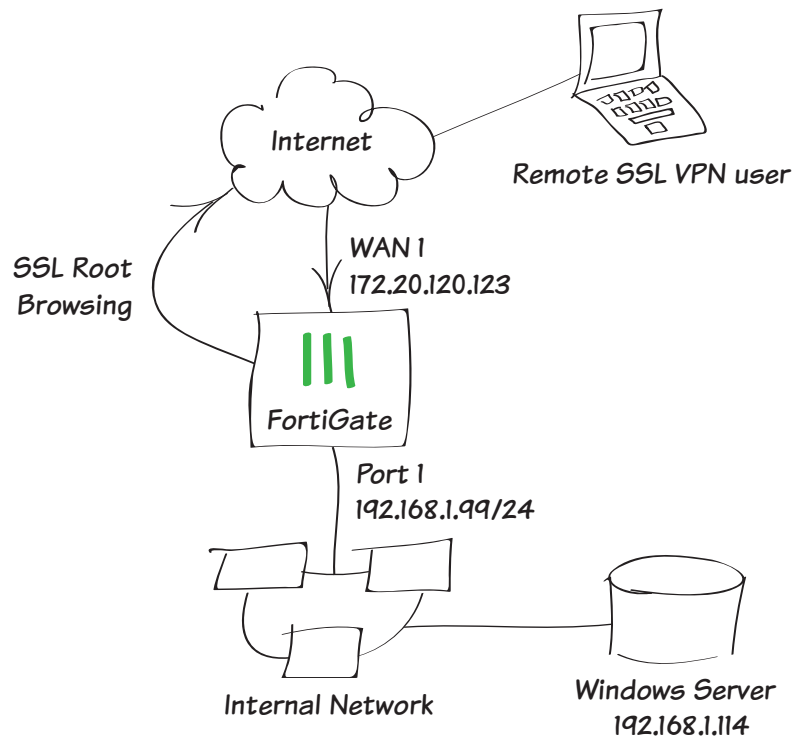


Providing remote users with access using SSL VPN

This example provides remote users with access to the corporate network using SSL VPN and connect to the Internet through the corporate FortiGate unit. During the connecting phase, the FortiGate unit will also verify that the remote user's antivirus software is installed and current.

1. Creating an SSL VPN tunnel for remote users
2. Creating a user and a user group
3. Adding an address for the local network
4. Adding security policies for access to the Internet and internal network
5. Setting the FortiGate unit to verify users have current AntiVirus software
6. Results



1. Creating an SSL VPN tunnel for remote users

Go to **VPN > SSL > Portals**.

Edit the full-access portal.

The full-access portal allows the use of tunnel mode and/or web mode. In this scenario we are using both modes.

Enable Split Tunneling is *not* enabled so that all Internet traffic will go through the FortiGate unit and be subject to the corporate security profiles.

full-access

☒ Enable Tunnel Mode

☐ Enable Split Tunneling

Source IP Pools

SSLVPN_TUNNEL_ADDR1

☒ Enable IPv6 Tunnel Mode

☐ Enable IPv6 Split Tunneling

Source IPv6 Pools

SSLVPN_TUNNEL_IPv6_ADDR1

Client Options

☐ Save Password

☐ Auto Connect

☐ Always Up (Keep Alive)

☒ Enable Web Mode

Portal Message

Welcome to SSL VPN Service

Theme

Blue

Page Layout

☒ Include Status Information

☒ Include Connection Tool

☒ Include FortiClient Download

☒ Prompt Mobile Users to Download FortiClient Application

☐ Include Login History

☒ Enable User Bookmarks

Predefined Bookmarks

Create New

Edit

Delete

Name	Type	Location	Description
No matching entries found			

☐ Limit Users to One SSL-VPN Connection at a Time

OK

Cancel

Select **Create New** in the **Predefined Bookmarks** area to add a bookmark for a remote desktop link/connection.

Bookmarks are used as links to internal network resources.



You must include a username and password. You will create this user in the next step, so be sure to use the same credentials.

New Bookmark

Category

Remote Desktop

Name

Windows Server

Type

RDP

Host

192.168.1.114

Screen Width

1024

Screen Height

768

Full Screen Mode

☒

Username

twhite

Password

.....

Keyboard Layout

English, US.

Description

OK

Cancel

2. Creating a user and a user group

Go to **User & Device > User > User Definition**.

Add a remote user with the User Creation Wizard (in the example, 'twhite', with the same credentials used for the predefined bookmark).

The image displays four sequential screenshots of the User Creation Wizard interface:

- Step 1: Choose User Type** - Shows radio buttons for Local User, Remote RADIUS User, Remote TACACS+ User, and Remote LDAP User. The 'Local User' option is selected.
- Step 2: Specify Login Credential** - Shows input fields for User Name (twhite) and Password (masked with dots).
- Step 3: Provide Contact Info** - Shows input fields for Email Address (twhite@example.com), Phone Number (555555555), and Service Type (FortiGuard Messaging Service).
- Step 4: Provide Extra Info** - Shows checkboxes for Enable, Two-factor Authentication, and User Group. The 'Enable' checkbox is checked.

Go to **User & Device > User > User Groups**.

Add the user 'twhite' to a user group for SSL VPN connections.

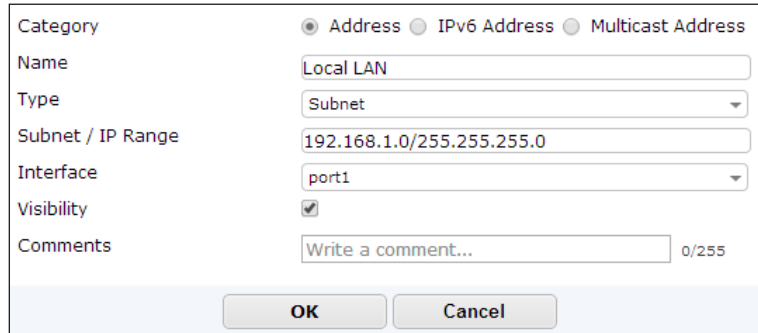
The image shows the User Groups configuration window:

- Name:** sslvpn_group
- Type (RSSO):** Firewall (selected), Fortinet Single Sign-On (FSSO), Guest, RADIUS Single Sign-On
- Members:** twhite (added)
- Remote groups:** A table with columns 'Remote Server' and 'Group Name'. It shows 'No matching entries found'.

3. Adding an address for the local network

Go to **Policy & Objects > Objects > Addresses**.

Add the address for the local network. Set **Subnet / IP Range** to the local subnet and set **Interface** to an internal port.



The screenshot shows the 'Add Address' dialog box in FortiGate. The 'Category' is set to 'Address'. The 'Name' is 'Local LAN'. The 'Type' is 'Subnet'. The 'Subnet / IP Range' is '192.168.1.0/255.255.255.0'. The 'Interface' is 'port1'. The 'Visibility' checkbox is checked. The 'Comments' field is empty. The 'OK' and 'Cancel' buttons are at the bottom.

4. Adding security policies for access to the Internet and internal network

Go to **Policy & Objects > Policy > IPv4**.

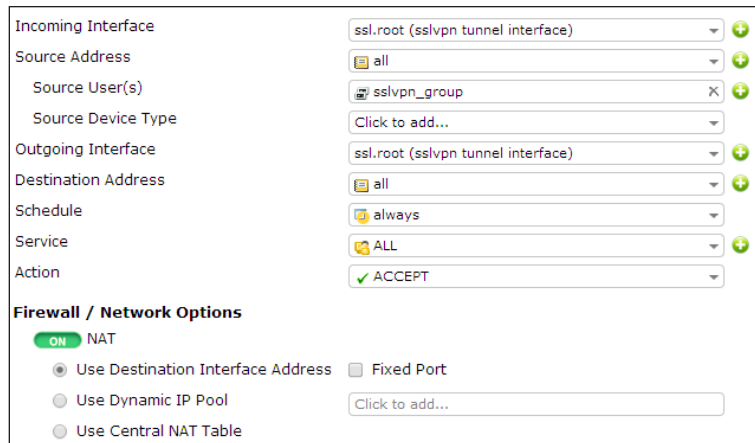
Add a security policy allowing access to the internal network through the *ssl.root* VPN tunnel interface.

Set **Incoming Interface** to **ssl.root**.

Set **Source Address** to **all** and select the **Source User** group you created in step 2.

Set **Outgoing Interface** to **ssl.root**, so that VPN traffic can flow between the remote user and the FortiGate.

Set **Destination Address** to **all**, enable **NAT**, and configure any remaining firewall and security options as desired.



The screenshot shows the 'Add Policy' dialog box in FortiGate. The 'Incoming Interface' is 'ssl.root (sslvpn tunnel interface)'. The 'Source Address' is 'all'. The 'Source User(s)' is 'sslvpn_group'. The 'Source Device Type' is 'Click to add...'. The 'Outgoing Interface' is 'ssl.root (sslvpn tunnel interface)'. The 'Destination Address' is 'all'. The 'Schedule' is 'always'. The 'Service' is 'ALL'. The 'Action' is 'ACCEPT'. The 'Firewall / Network Options' section is expanded, showing 'NAT' is enabled. The 'Use Destination Interface Address' radio button is selected. The 'Fixed Port' checkbox is unchecked. The 'Use Dynamic IP Pool' and 'Use Central NAT Table' radio buttons are unselected. The 'Click to add...' button is visible.

Add a second security policy allowing SSL VPN access to the Internet.

For this policy, **Incoming Interface** is set to **ssl.root** and **Outgoing Interface** is set to **wan1**.

Incoming Interface	ssl.root (sslvpn tunnel interface)
Source Address	all
Source User(s)	Click to add...
Source Device Type	Click to add...
Outgoing Interface	wan1
Destination Address	all
Schedule	always
Service	ALL
Action	ACCEPT

5. Setting the FortiGate unit to verify users have current AntiVirus software

Go to **System > Status > Dashboard**.

In the **CLI Console** widget, enter the commands on the right to enable the host to check for compliant AntiVirus software on the remote user's computer.

```
# config vpn ssl web portal
(portal) # edit full-access
(full-access) # set host-check av
(full-access) # end
```

6. Results

Log into the portal using the credentials you created in step 2.

login - Internet Explorer, optimized for Bing and MSN

https://172.20.123.10443/remote/login Certificate Error

login

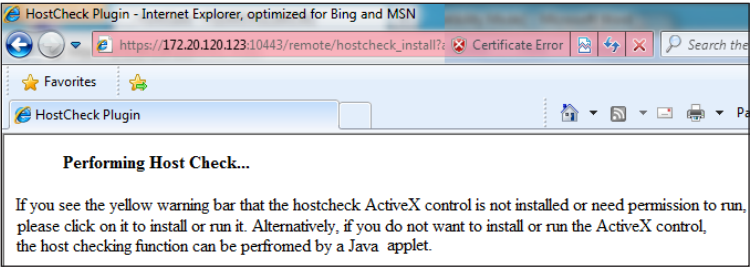
Please Login

Name: twhite

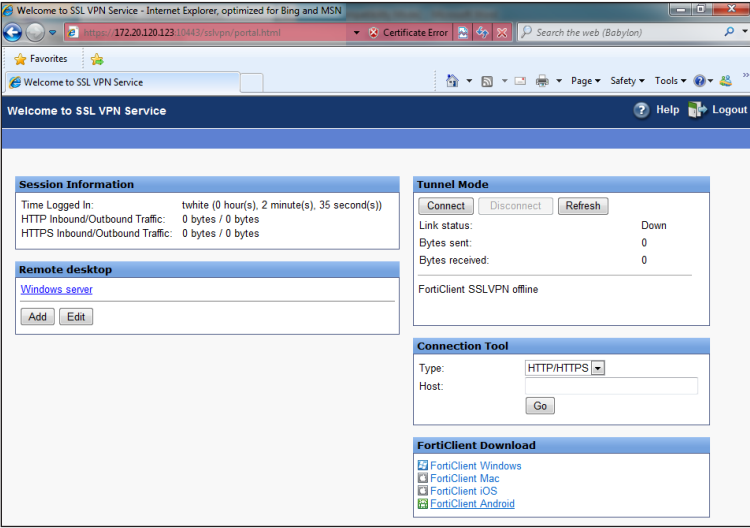
Password:

Login

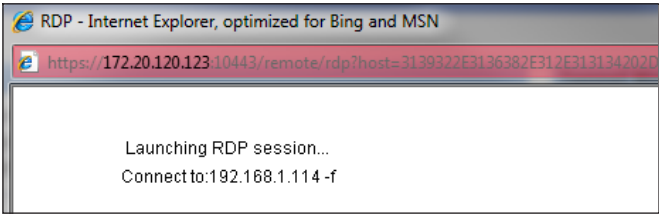
The FortiGate unit performs the host check.



After the check is complete, the portal appears.






Select the bookmark **Remote Desktop** link to begin an RDP session.



Go to **VPN > Monitor > SSL-VPN Monitor** to verify the list of SSL users. The Web Application description indicates that the user is using web mode.

No.	User	Source IP	Begin Time	Descrip
1	twwhite	172.20.120.23	Wed Apr 17 11:41:06 2013	
Subsession		Web Application:RDP 192.168.1.114		

Go to **Log & Report > Traffic Log > Forward Traffic** and view the details for the SSL entry.

Dst	192.168.1.114	Virtual Domain	root
Received	85591	Source Country	Reserved
Sent / Received	8.71 KB / 83.58 KB	Duration	36
Sent	8923	Application Details	
Group	N/A	Service	RDP
Protocol	6	User	 twhite
Destination Country	Reserved	Dst Port	3389
roll	65389	Status	✓
Timestamp	Wed Apr 17 14:13:11 2013	Tran Display	noop
Sequence Number	2700	Policy ID	11
Src Interface	wan1	Src	 twhite (172.20.120.23)
VPN	sslvpn_web_mode	Sent Packets	71
Level	notice 	VPN Type	sslvpn
Src Port	53712	Log ID	13
Sub Type	forward	Threat	
Received Packets	98	Date/Time	14:13:11 (Wed Apr 17 14:13:11 2013)
Dst Interface	port1		

In the **Tunnel Mode** widget, select **Connect** to enable the tunnel.

Tunnel Mode

Connect

Disconnect

Refresh

Link status:

Up

Bytes sent:

46865


Bytes received:


118096

FortiClient SSLVPN connected to server

Select the bookmark **Remote Desktop** link to begin an RDP session.

RDP - Internet Explorer, optimized for Bing and MSN

 https://172.20.120.123:10443/remote/rdp?host=31393

 Certificate Error

Launching RDP session...




Connect to:192.168.1.114 -f

Go to **VPN > Monitor > SSL-VPN Monitor** to verify the list of SSL users.

The tunnel description indicates that the user is using tunnel mode.












No.	User	Source IP	Begin Time	D
1	twhite	172.20.120.23	Wed Apr 17 11:41:06 2013	
	Subsession		Tunnel IP:10.212.134	

Go to **Log & Report > Traffic Log > Forward Traffic** and view the details for the SSL entry.


Dst	192.168.1.114	Virtual Domain	root
Received	326664	Source Country	Reserved
Sent / Received	54.36 KB / 319.01 KB	Duration	83
Sent	55665	Application Details	
Group	N/A	Service	RDP
Protocol	6	User	 twhite
Destination Country	Reserved	Dst Port	3389
roll	65389	Status	✓
Timestamp	Wed Apr 17 14:17:15 2013	Tran Display	noop
Sequence Number	3618	Policy ID	11
Src Interface	wan1	Src	 twhite (172.20.120.23)
VPN	sslvpn_web_mode	Sent Packets	329
Level	notice 	VPN Type	sslvpn
Src Port	53820	Log ID	13
Sub Type	forward	Threat	
Received Packets	407	Date/Time	14:17:15 (Wed Apr 17 14:17:15 2013)
Dst Interface	unknown-0		

Go to **Log & Report > Traffic Log > Forward Traffic**.

Internet access occurs simultaneously through the FortiGate unit.

 Refresh  Download Raw Log					
#	▼ Date/Time	▼ Src Interface	▼ Dst Interface	▼ Src	▼ Dst
▶ 1	14:26:05	ssl.root	wan1	10.212.134.200	 74.125.133.95
2	14:26:04	ssl.root	wan1	10.212.134.200	 173.194.77.94
3	14:26:04	ssl.root	wan1	10.212.134.200	 173.194.43.79
4	14:26:03	ssl.root	wan1	10.212.134.200	 66.171.121.34 (fortinet.co
5	14:25:57	ssl.root	wan1	10.212.134.200	 74.121.50.17 (www.pages
6	14:25:44	ssl.root	wan1	10.212.134.200	 208.91.113.212
7	14:25:40	ssl.root	wan1	10.212.134.200	192.168.55.30
8	14:25:40	ssl.root	wan1	10.212.134.200	192.168.55.30
9	14:25:40	ssl.root	wan1	10.212.134.200	192.168.55.30
10	14:24:39	ssl.root	wan1	10.212.134.200	 213.199.179.159
11	14:24:37	ssl.root	wan1	10.212.134.200	 213.199.179.159
12	14:24:37	ssl.root	wan1	10.212.134.200	 132.246.2.6 (www.msftncs

Select an entry to view more information.

Dst	 66.171.121.34 (fortinet.com)	Virtual Domain	root
Received	938	Source Country	Reserved
Src NAT IP	172.20.120.123	Sent / Received	535 B / 938 B
Duration	17	Sent	535
Src NAT Port	54165	Application Details	
Service	HTTP	Protocol	6
Destination Country	United States	Dst Port	80
roll	65389	Status	close
Timestamp	Wed Apr 17 14:26:03 2013	Tran Display	snat
Sequence Number	8096	Policy ID	8
Src Interface	ssl.root	Src	10.212.134.200
Sent Packets	6	Level	notice 